




Security Management Infrastructure: Session Key Management Protocols (and some other stuff)

National Security Agency
INFOSEC Research and Technology Office
Computer Security Research Division

Phone: 301-688-0847

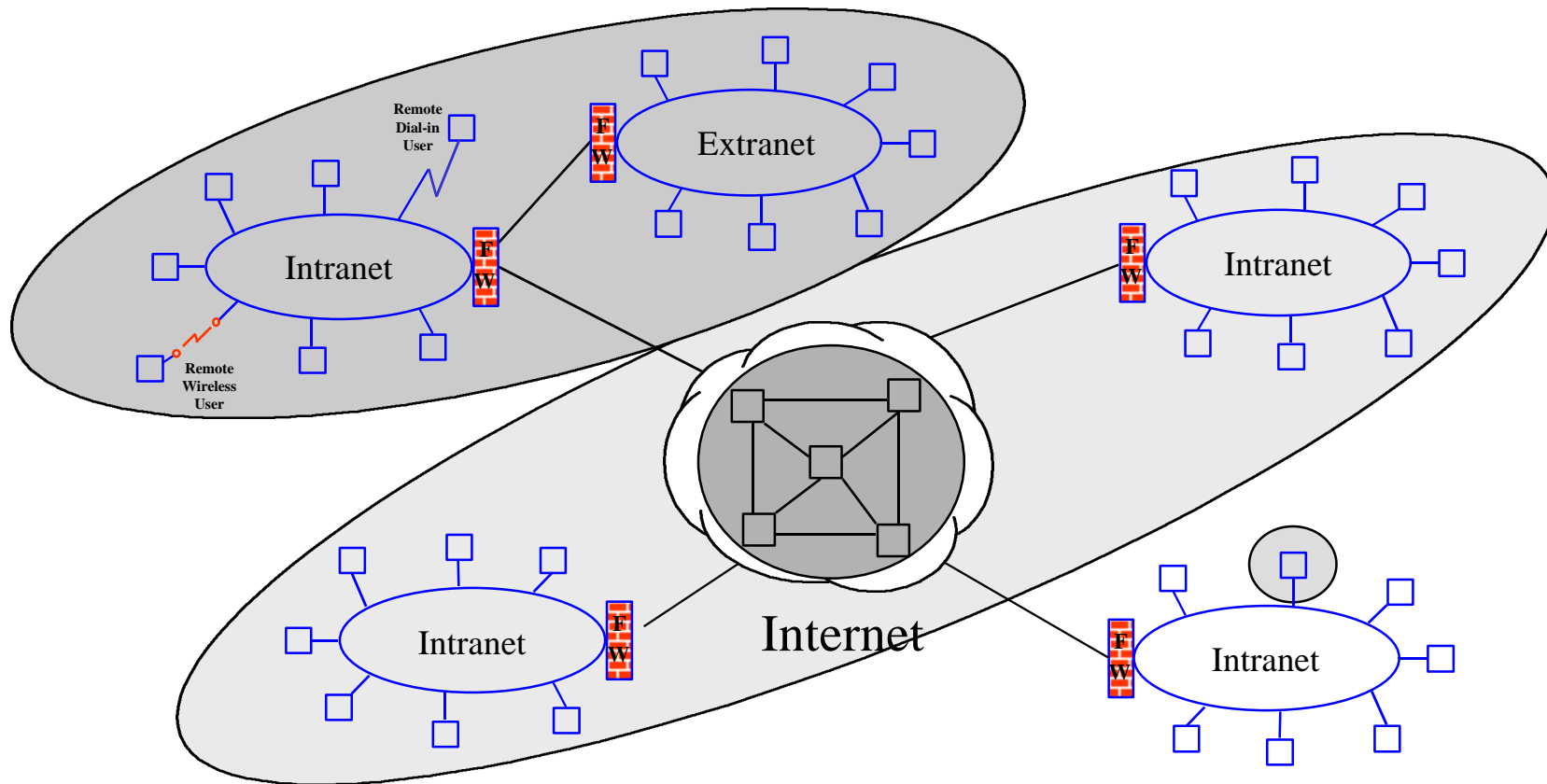
POC: Douglas Maughan

E-mail: wdm@tycho.ncsc.mil

wdmpc@epoch.ncsc.mil - MS  's



Network Security Management Infrastructure Diagram



3/30/98

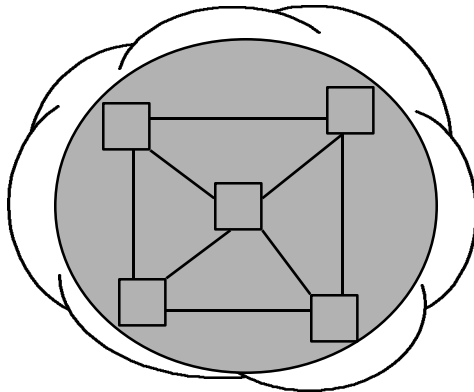


SMI Components

- Infrastructure View
- Internet View
- Intranet View
 - Extranet
 - Remote Users
- Host View



Infrastructure View

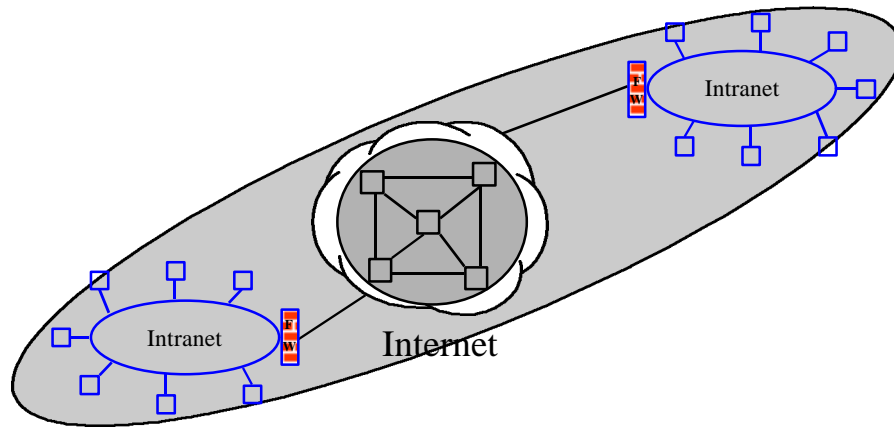


Internet

- **Routing**
 - Secure Routing Protocols
- **Multicast Communications**
 - Key Management
- **Network Management**
 - Secure Exchange of Management Info.
 - Applicable to Intranet/Internet Views
- **Intrusion Detection**
 - Support to Users
 - Ties to Network Management



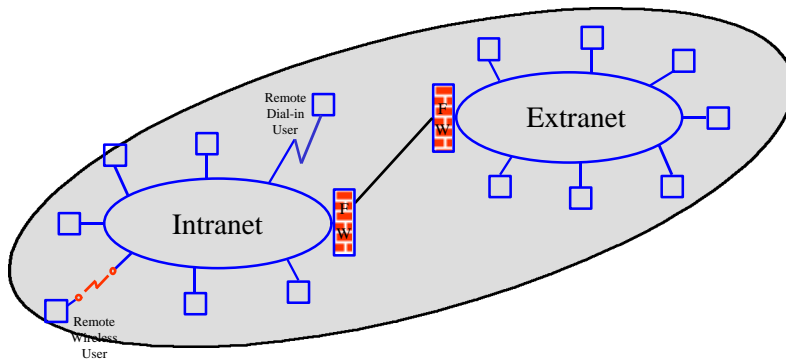
Internet View



- **Security Policies**
 - Across Domains; Negotiate
- **Identification**
 - Host-Host; User-User
- **Infrastructure(s)**
 - Public Key
 - Certificate Mgmt.
- **Security Negotiation**
 - Security Mechanisms
- **Security Protocols**
- **Intrusion Detection**



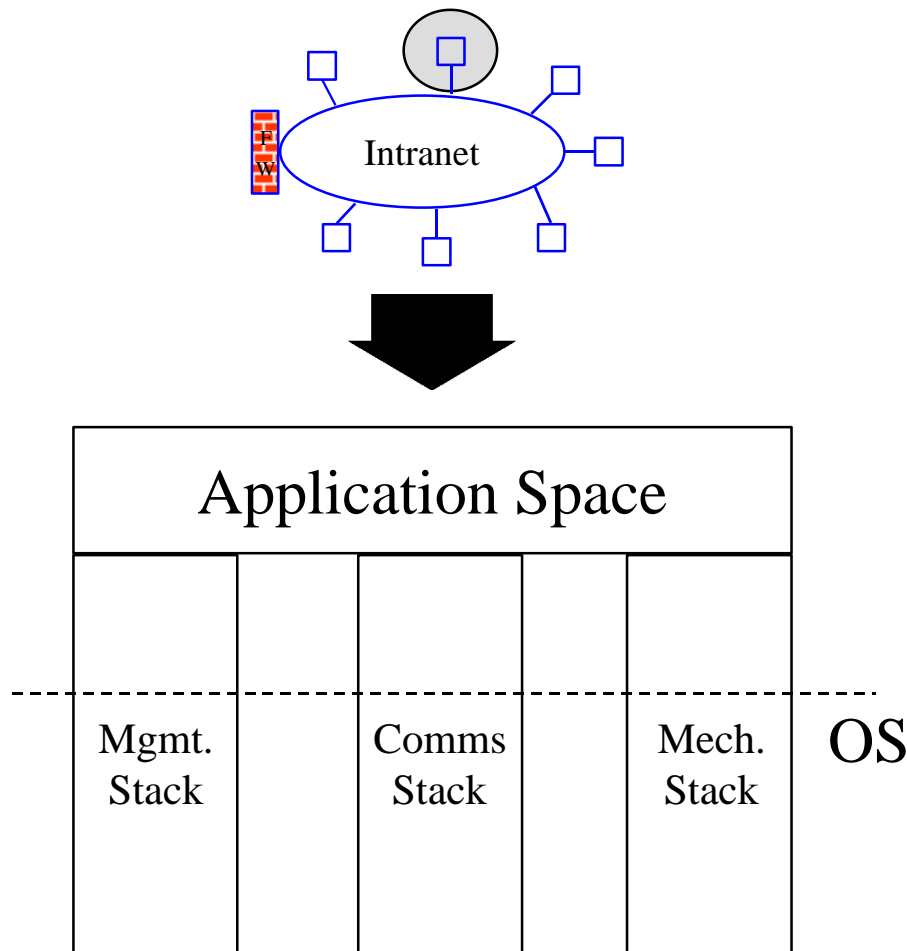
Intranet (and Extranet) View



- **Security Policies**
 - Comms with Extranet and Remote Users
- **Identification**
 - Host-Host; User-User
- **Infrastructure(s)**
 - Public Key
 - Certificate Mgmt.
- **Security Negotiation**
 - Security Mechanisms
- **Security Protocols**
- **Intrusion Detection**



Host View



- **Security Policies**
 - H2M Translation; Proper Enforcement by OS
- **Identification**
 - User-Host
- **Application(s)**
 - Security
 - Non-Security
- **Comms Stack**
- **TCB / Trusted OS**
- **CAPIs**
- **Intrusion Detection**



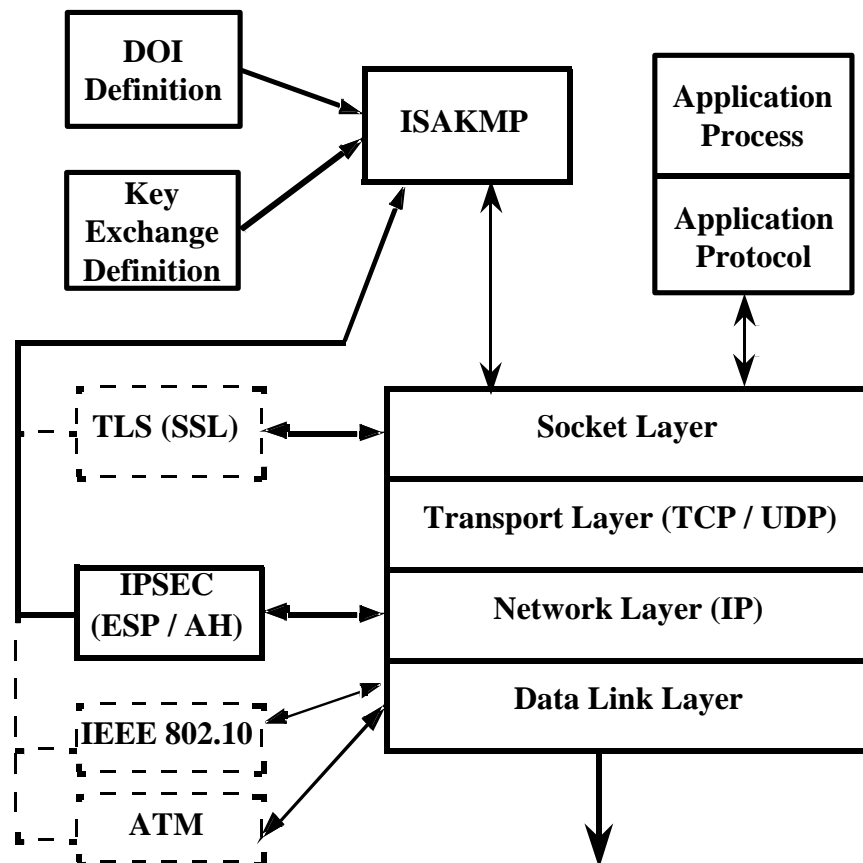
Internet Security Association and Key Management Protocol (ISAKMP)

- NSA submission to the IETF for future Internet Key Management
 - Work started in December 1994
 - Selected as the mandatory-to-implement key management for IPv6; optional for IPv4 (Sept. 1996)
- IETF Key Management Requirements
 - Security Associations & Management
 - Security Attribute Negotiation; Mechanism Independence
 - Authentication (requires additional infrastructure)
 - Public Key Cryptography



ISAKMP (continued)

- Architecture



3/30/98



ISAKMP (continued)

- Security Association Management
 - Independent Security Attribute Definition
 - SA presentation --> Type/Length/Value Encoding
 - Supports Multiple Protocols Requiring Security
- Authentication
 - Supports user or host oriented authentication
 - Supports multiple certificate formats and authorities
- Public Key Cryptography
 - Independent of specific key exchange (supports all)
 - Currently, Internet Key Exchange (IKE)



ISAKMP (continued)

- Negotiation Phases
 - Phase 1 establishes secure channel between ISAKMP's
 - Phase 2 establishes SA between protocols (e.g. IPSEC)
- ISAKMP Messages consist of Payloads
 - Security Association, Proposal, Transform, Key Exchange, Identification, Hash, Nonce, Signature, Certificate, Certificate Request, Notify, Delete
- ISAKMP Exchanges
 - Payloads designed to provide a specific security service
 - Authentication-Only, Aggressive, Base, Identity Protect, Informational



ISAKMP (continued)

- Current Status
 - Internet-Draft: draft-ietf-ipsec-isakmp-09.ps, .txt
 - IP Security Domain of Interpretation
 - Internet-Draft: draft-ietf-ipsec-ipsec-doi-08.txt
 - Key Exchange
 - Internet-Draft: draft-ietf-ipsec-isakmp-oakley-07.txt
- Interoperability Opportunities
 - SSH (Finland) - www.ssh.fi
 - NIST - Soon to be available as part of IPSEC-WIT
 - Recent AIAG-sponsored interoperability testing



On Another Note

NSA
Security Management Infrastructure
Research Project Review
and
(dare I say) Research Solicitation



Current SMI Projects

- Internet Security Protocols (ISP)
- Key Management Infrastructure (KMI)
- Multicast Security Key Management (MSKM)
- Network Security Management (NSM)
- Secure Internet Protocol Analysis (SIPA)

- Are there “critical” areas we are missing?



Internet Security Protocols

(support of All Views)

- ISAKMP Design, Development, and Testing
 - Design and Document Editing In-House
 - Code being developed by TeleniX
- Modeling and Simulation of ISAKMP
 - Performance and scalability using TeleniX's SimuNet
- ISAKMP/Fortezza Integration
 - Incorporate Fortezza mechanisms into IP Sec. Arch.
- Policy-Based Dynamic Security Management
 - Development of IPSEC policy negotiation mechanisms
 - DARPA/ITO co-funded work at BBN



Internet Security Protocols (cont'd)

(support of All Views)

- IPSEC Development and Support
 - Sponsor IPSEC development at NIST
 - WWW-based IPSEC Testing (IPSEC-WIT)
- Enforcing Access Control within IPv6
 - IPv6 Packet-level access control scheme
 - Univ. of Florida (NSA University Research Program)
- Domain Name System Security (DNSSEC)
 - Add additional proposed IETF mechanisms to existing TIS implementation
 - Research under consideration - not funded yet



Key Management Infrastructure

(support of Intranet and Internet Views)

- Key Generation Techniques (In- House)
- Certificate Management
 - CA Scalability (work with MIT Lincoln Labs)
 - Certificates for Access Control (In-House)
 - Certificates for binding Users/Public Keys and Servers/CAs (In-House)
 - Using X.509 Attribute Certificates in Low-Bandwidth Environments (work with MITRE-CECOM)
 - Certificate Revocation (In-House)
 - Cross Certification (In-House)



Multicast Security Key Management

(support of Infrastructure View)

- Multicast Issues and Architectures
 - Internet-Draft: draft-wallner-key-arch-00.txt
 - Architecture for dealing with compromised users in a multicast environment (Logical Key Hierarchy {LKH})
 - Supported by contract with Sparta to do multicast security requirements analysis and follow-on prototype implementation
- Coordination with DARPA work
 - Dynamic Cryptographic Context Management (DCCM)
 - One-Way Function Trees (OFT) - different approach than LKH
 - DARPA/ITO co-funded work at TIS



Network Security Management

(support of Infrastructure View)

- DARPA/ISO Information Assurance Security Architecture Support
 - A Security Management Foundation for the GCCS LES Reference Architecture
 - Development of a Security Management Workstation within the subject architecture (co-funded work being done by TIS)
- Develop SNMPv3 Reference Implementation
 - Based on existing IETF RFCs 2271-2275
 - Initial SW & Security-enhanced version to be released
 - Support Standardization and Interoperability Testing



Secure Internet Protocol Analysis

(support of All Views)

- Education and evaluation of NRL Analyzer tool
 - Sponsor course development and presentation for NRL Analyzer tool (Cathy Meadows, developer)
- Research into automated analysis methodologies
 - Formal methods research has been less than successful
 - Are Model Checking techniques adequate?
- Protocol Vulnerability Analysis (In-House)
 - FY98: PPP, DNSSEC, S/MIME, SNMP
 - FY99: DHCP, MobileIP, RSVP, IKE



Research Solicitation

- Limited Resources available to all
- Interested in partnering with DoE researchers
- Areas of Interest (willing to expand)
 - Certificate Management Infrastructure
 - Certificate Revocation
 - Cross Certification
 - Multicast Security - Routing
 - Multicast Security - Non-Cryptographic Techniques
- Available Money: FY98: \$200K - \$300K
FY99: \$500K - \$1M



CMI - Certificate Revocation

- Critical part of infrastructure is the architecture piece associated with certificate revocation
- Current methods of performing certificate revocation are Certificate Authorities (CAs) maintain Certificate Revocation Lists (CRLs)
- Current CRL methods include: (1) on-line validation {OCSP}; (2) “push” CRLs {PKIX}; and (3) long-term offline techniques
- Should consider topics like high assurance, key recovery, and role-based access control



CMI - Cross Certification

- Critical part of infrastructure is the ability to verify security information from a different security domain through cross certification
- Future Internet infrastructure will support multiple certificate infrastructures (e.g. X.509, DNSSEC, PGP, SPKI) and cross certification is a MUST
- Should address issues associated with domain security policies, address mapping policies, certificate formats, security domain authority trust, certificate revocation



Multicast Security - Routing and Non-Cryptographic Techniques

- Major Internet infrastructure communication component lacking “clear” security direction
- To date, most research aimed at the key management problem for large multicast groups; some routing has been done (e.g. CBT, PIM)
- Significant problems include group initialization, sender-initiated group rekey, revocation distribution
- Need to consider other techniques (non-crypto) for potential - security, performance, scalability



Summary

- Context of Security Management Infrastructure
- Internet Security Association and Key Management Protocol (ISAKMP) Review/Status
- Review of NSA Security Management Infrastructure Research Projects
- Research Solicitation
- “Only working on the tip of the SMI Iceberg”



Contact Info


National Security Agency
INFOSEC Research and Technology Office
Computer Security Research Division

Phone: 301-688-0847

Fax: 301-688-0255

POC: Douglas Maughan

E-mail: wdm@tycho.ncsc.mil

wdmpc@epoch.ncsc.mil - MS  's